Journal of Algebra 569 (2021) 658–680

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

On properties of translation groups in the affine general linear group with applications to cryptography ☆

Marco Calderini [a,*], Roberto Civino [b], Massimiliano Sala [c]

[a] Department of Informatics, University of Bergen, Norway
[b] DISIM, University of l'Aquila, Italy
[c] Department of Mathematics, University of Trento, Italy

ARTICLE INFO

Article history:
Received 29 April 2020
Available online 24 November 2020
Communicated by Derek Holt

Keywords:
Translation group
Affine group
Block ciphers
Cryptanalysis

ABSTRACT

The affine general linear group acting on a vector space over a prime field is a well-understood mathematical object. Its elementary abelian regular subgroups have recently drawn attention in applied mathematics thanks to their use in cryptography as a way to hide or detect weaknesses inside block ciphers. This paper is focused on building a convenient representation of their elements which suits better the purposes of the cryptanalyst. Several combinatorial counting formulas and a classification of their conjugacy classes are given as well.

☆ This research was partially funded by the Italian Ministry of Education, Universities and Research (MIUR), with the project PRIN 2015TW9LSR "Group theory and applications". Roberto Civino is partially funded by the Centre of Excellence EX-EMERGE at University of L'Aquila.

* Corresponding author.
E-mail addresses: marco.calderini@uib.no (M. Calderini), roberto.civino@univaq.it (R. Civino), massimiliano.sala@unitn.it (M. Sala).

https://doi.org/10.1016/j.jalgebra.2020.10.034

1. Introduction

The group of the translations of a vector space over a prime field is an elementary abelian regular subgroup of the corresponding symmetric group, and its normaliser, the affine general linear group, is a well-understood mathematical object. Regular subgroups of the affine group and their connections with algebraic structures, such as radical rings [16] and braces [19], have already been studied in several works [18,24,27,28]. More recently, elementary abelian regular groups have been used in cryptography to define new operations on the message space of a block cipher and to implement statistical and group theoretical attacks [13,15,20]. All these objects are well-known to be conjugated to the translation group, but this fact does not provide a simple description and representation of their elements which is useful to the cryptanalyst. For this reason, we address the problem of giving a convenient matrix representation of some elementary abelian regular subgroups of the affine groups and, in some cases, we classify them in terms of their conjugacy classes. The idea behind the cryptographic attack resulting from this work is the one of using alternative group structures on the message space of a block cipher to detect a bias in the distribution of the encrypted messages, as we will describe in the following section in more detail. Although the approach of using alternative operations in place of the XOR (the usual sum over a binary vector space) is not new [1,7], the idea of using groups isomorphic to the translation group was never considered.

1.1. Organisation of the paper

The paper is organised as follows. In Section 2 we introduce the notation and present the main focus of the work, also providing a description of the idea which is behind the use of translation groups in cryptography. In Section 3 we present our main result, i.e. Theorem 3.11, which proves a description of the translation groups useful in block ciphers cryptanalysis. Section 4 is mainly devoted to the case of binary fields, to combinatorial aspects of the topic and to a classification of conjugacy classes in low dimension. In Theorem 4.1 and Theorem 4.7 we provide a bound on the numbers of groups as in Theorem 3.11.

2. Preliminaries

Let us start by introducing the notation used throughout this work.

Let p be a prime number, $n \geq 2$ a positive integer and $V \stackrel{\text{def}}{=} (\mathbb{F}_p)^n$ be the n-dimensional vector space over $\mathbb{F}_p$. The i-th component of the vector $v \in V$ is denoted by $v^i \in \mathbb{F}_p$. The canonical basis of V is composed by the vectors $\{e_i\}_{i=1}^n$, where $e_i^j = 1$ if and only if $i = j$, otherwise it is 0. The vector subspace generated by vectors $v_1, \ldots, v_m \in V$ is denoted by $\mathrm{Span}\{v_1, \ldots, v_m\}$, where $m \geq 1$. Let $\mathrm{Sym}(V)$ be the group of all the permutations on V. In this paper we use postfix notation for function evaluation, i.e. if $g \in \mathrm{Sym}(V)$ and $v \in V$ we write vg to mean $g(v)$. The identity of $\mathrm{Sym}(V)$ is denoted by 1_V and if

$g_1, \ldots, g_m \in \mathrm{Sym}(V)$, where $m \geq 1$, we denote by $\langle g_1, \ldots, g_m \rangle$ the group they generate. Let $\mathrm{GL}(V)$ be the general linear group on V, i.e. the group of the linear permutations of V, and let us denote by T the group of all the translations on V, i.e. $T \stackrel{\text{def}}{=} \{\sigma_a \mid a \in V, \sigma_a : V \to V, x \mapsto x + a\}$. Then, let the affine general linear group $\mathrm{AGL}(V)$, the normaliser of T in the symmetric group, be represented as $\mathrm{AGL}(V) = \mathrm{GL}(V) \ltimes T$. Let $(\mathbb{F}_p)^{i \times j}$ denote the set of all matrices with entries over $\mathbb{F}_p$ with i rows and j columns. The identity matrix is denoted by 1_n.

In this work we will also use some basic ring-theoretical notions that are summarised here for the convenience of the reader. Let R be a ring. An element $r \in R$ is called *nilpotent* if $r^m = 0$ for some $m \geq 1$ and it is called *unipotent* if $r - 1$ is nilpotent, i.e. $(r-1)^m = 0$ for some $m \geq 1$. Analogously, if $H \leq \mathrm{GL}(V)$ is a subgroup of unipotent permutations, then H is called unipotent. An element $M \in \mathrm{GL}(V)$ is said *upper unitriangular in a basis* $\{v_1, \ldots, v_n\}$ on V if and only if $v_i M - v_i \in \mathrm{Span}\{v_{i+1}, \ldots, v_n\}$ for all $1 \leq i \leq n$. The map M is called *upper unitriangular* if it is upper triangular with respect to the canonical basis. The group of upper unitriangular linear maps is here denoted by $\mathcal{U}(V)$.

The idea of the cryptographic application of this study is described in the following section.

2.1. Motivation and links to the theory of block ciphers

Let $\mathcal{T} < \mathrm{Sym}(V)$ be elementary abelian regular. As already mentioned, from a result due to Dixon [23] (see also [5] for an easy proof), there exists $g \in \mathrm{Sym}(G)$ such that $\mathcal{T} = T^g \stackrel{\text{def}}{=} g^{-1}Tg$. Since $\mathcal{T}$ inherits from T its regularity, and recalling that for each $a \in V$ we denoted by $\sigma_a \in T$ the translation sending 0 to a, it is possible to represent $\mathcal{T} = \{\tau_a \,|\, a \in V\}$, where the map τ_a is the unique in $\mathcal{T}$ sending 0 to a. Once this labelling is established, it is possible to define an additive law $\circ$ on V by letting for each $a, b \in V$ $a \circ b \stackrel{\text{def}}{=} a\tau_b$. It is easy to check that $(V, \circ)$ is an abelian group whose corresponding translation group is $T_\circ = \mathcal{T}$. Moreover, letting the multiplication of a vector by a non-zero element $s \in \mathbb{F}_p$ be defined as

$$sv \stackrel{\text{def}}{=} \underbrace{v \circ \cdots \circ v}_{s},$$

it is easily checked that if $s, t \in \mathbb{F}_p$ and $v, w \in V$, then

$$s(v \circ w) = sv \circ sw,$$
$$(s + t)v = sv \circ tv,$$
$$(st)v = s(tv),$$

and $pv = 0$ since $\mathcal{T}$ is elementary. This proves that $(V, \circ)$ is a vector space over $\mathbb{F}_p$, and since $|V| < \infty$, $(V, \circ)$ and $(V, +)$ are isomorphic vector spaces. We will denote by

$\mathrm{AGL}(V,\circ) \stackrel{\text{def}}{=} \mathrm{AGL}(V)^g$ the normaliser of $T_\circ = \mathcal{T}$ and by $\mathrm{GL}(V,\circ)$ the stabiliser of $\{0\}$ in $\mathrm{AGL}(V,\circ)$. Since in this paper we will always deal with different operations at the same time, for sake of clarity we will sometimes denote T as T_+, $\mathrm{AGL}(V)$ by $\mathrm{AGL}(V,+)$ and $\mathrm{GL}(V)$ by $\mathrm{GL}(V,+)$.

The idea of using an application of the group-theoretical study of translation groups to block ciphers comes from the fact that the translation is the standard way the user introduces its *key* in the encryption process (in cryptographic terms, the key is XOR-ed to the message). In order to explain this fact and to let the reader figure out the potential attacks coming from alternative translation groups, we will give here a little and self-contained introduction to block ciphers. A *block cipher* on the message space V is a set of many invertible function in $\mathrm{Sym}(V)$, called *encryption functions*. Popular examples may be found e.g. in [11,22]. Each encryption function is of the type of

$$\rho\sigma_{k_1}\rho\sigma_{k_2}\dots\rho\sigma_{k_r},$$

where $\rho \in \mathrm{Sym}(V)$ and the parameter $r \in \mathbb{N}$ are fixed by the designer and made publicly available, and the sequence $(k_1, k_2, \dots k_r) \in V^r$ represents the *encryption key* chosen by the user. Once the key $(k_1, k_2, \dots k_r)$ and the message $m \in V$ to be sent are chosen by the sender, it delivers $m\rho\sigma_{k_1}\rho\sigma_{k_2}\dots\rho\sigma_{k_r}$ to the receiver. If the receiver is entitled to recover the message, i.e. if it knows the secret key, it can apply the inverse of the encryption function and obtain the original message m. The security of this process, i.e. the inability of a non-authorised party to recover the message, strongly relies on the way the function ρ is designed. Indeed, the process of designing ρ is one of the most important phases in the definition of a block cipher, and it is usually carried out in order to guarantee that the obtained block cipher is resistant against each known attack (e.g. linear [25] and differential [8] cryptanalysis). Giving details and properties that the function ρ has to satisfy is out of the scope of this work, for whose purposes is enough to know that a minimum and crucial requirement is that $\rho \notin \mathrm{AGL}(V)$. As a matter of fact, the farthest it lies from the affine group, the better. This guarantees that the group $\langle \rho, T \rangle$, called *the group of the round functions*, is not the affine group $\mathrm{AGL}(V)$. Such a group, introduced in [21] for the first time, has been carefully studied ever since researchers have shown that some of its properties can reveal weaknesses of the cipher [2–4,6,17,26,29,31,32]. Although it is rather easy to select ρ such that $\langle \rho, T \rangle$ is different from $\mathrm{AGL}(V)$, it not as easy to prove that $\langle \rho, T \rangle$ is not contained in any conjugate of $\mathrm{AGL}(V)$ in $\mathrm{Sym}(V)$. If this is the case, i.e. if there exists $g \in \mathrm{Sym}(V)$ such that $\langle \rho, T \rangle < \mathrm{AGL}(V)^g$, then there exists an operation $\circ$ such that

$$\langle \rho, T \rangle \leq \mathrm{AGL}(V,\circ), \tag{1}$$

which means that each encryption function is affine with respect to the operation $\circ$, a serious threat for the security of the cipher. A description of the attack that can be performed in this case is shown in [14]. Another example in this regard, i.e. a successful

attack against a block cipher which makes use of an operation as described above, can be found in [20]. For the reason explained before, since our interest is in determining if and when the group of the round functions is as in Eq. (1), we focus on investigating operations $\circ$ such that $T < \mathrm{AGL}(V, \circ)$. Such hypothesis is also decisive in the application studied in [20], where the classical differential attack (see e.g. [9,10]) is generalised to alternative operations. Moreover, we will always assume $T_\circ < \mathrm{AGL}(V)$, since it guarantees fast computation, crucial in the application to cryptanalysis. The related problem of determining conditions on $\rho \notin \mathrm{AGL}(V)$ which ensure that $\rho \in \mathrm{AGL}(V, \circ)$ for some operation $\circ$ is still open. Some partial results can be found in [13,15,20].

In the next section we will introduce our novel results and in particular we will describe all elementary abelian regular groups $T_\circ < \mathrm{AGL}(V, +)$ such that $T_+ < \mathrm{AGL}(V, \circ)$.

3. Abelian regular subgroups of the affine groups

Keeping in mind the construction of Sec. 2, we now focus on groups conjugated to T which are affine groups. A seminal work for this research is the paper [16], where the authors give an easy description of the abelian regular subgroups of the affine group in terms of commutative associative algebras that one can define on the vector space $(V, +)$. Here we summarise their main results. Recall that a *Jacobson radical ring* is a ring $(V, +, \cdot)$ such that $(V, \diamond)$ is a group, where the operation $\diamond$ defined as $a \diamond b = a + b + a \cdot b$, for each $a, b \in V$. Note that in general the operation $\diamond$ does not induce a vector space structure on V. The proof of the next result may be found in [16].

Theorem 3.1. *Let $\mathbb{K}$ be any (finite or infinite) field, and $(V, +)$ be a vector space of any dimension over $\mathbb{K}$. There is a one-to-one correspondence between*

1. *abelian regular subgroups of* $\mathrm{AGL}(V, +)$,
2. *commutative, associative $\mathbb{K}$-algebra structures $(V, +, \cdot)$ that one can impose on the vector space structure $(V, +)$, such that the resulting ring is radical.*

In this correspondence, isomorphism classes of $\mathbb{K}$-algebras correspond to conjugacy classes of abelian regular subgroups of $\mathrm{AGL}(V, +)$, *where the conjugation is under the action of* $\mathrm{GL}(V, +)$.

The correspondence mentioned in the previous result may be written explicitly, proceedings as follows. Let $\mathcal{T} < \mathrm{AGL}(V)$ be abelian and regular. Since $\mathcal{T}$ is regular, reasoning as in Sec. 2 its elements can be labelled as $\mathcal{T} = \{\tau_a \mid a \in V\}$. For each $a \in V$, from the hypothesis, there exists $M_{a,\mathcal{T}} \in GL(V, +)$ and $\sigma_b \in T_+$ for some $b \in V$ such that $\tau_a = M_{a,\mathcal{T}} \sigma_b$. In order to keep the notation lighter, $M_{a,\mathcal{T}}$ will be simply denoted by M_a. For any $a \in V$, let us define the map $\delta_a \stackrel{\text{def}}{=} M_a - 1_V$. Then, operation $\cdot$ defined on V by letting $x \cdot a = x\delta_a$ is such that the structure $(V, +, \cdot)$ is a commutative $\mathbb{K}$-algebra and the resulting ring is radical. Moreover, notice that $0\tau_a = a$ by definition,

then $a = 0\tau_a = 0M_a\sigma_b = b$, hence $\tau_a = M_a\sigma_a$ for each $a \in V$. Denoting by $\circ$ the operation induced by $\mathcal{T}$, let us now define the set

$$\Omega(\mathcal{T}) = \Omega_\circ \stackrel{\text{def}}{=} \{M_a \mid a \in V\} < \mathrm{GL}(V),$$

and denote by $T_\circ = \mathcal{T}$.

Proposition 3.2. *Let $\mathcal{T} < \mathrm{AGL}(V)$ be an elementary abelian regular subgroup. Then for each $a \in V$, $M_a \in \mathrm{GL}(V)$ has order p and it is unipotent. In particular $\Omega(\mathcal{T})$ is a unipotent subgroup of $\mathrm{GL}(V)$.*

Proof. Let $a \in V$. Since $\mathcal{T}$ is elementary, τ_a has order p, so $a{\tau_a}^{p-1} = 0$. For each $x \in V$ we get

$$x = x\tau_a^p = (xM_a + a){\tau_a}^{p-1} = (xM_a^2 + a\tau_a){\tau_a}^{p-2} = \ldots = xM_a^p + a{\tau_a}^{p-1},$$

therefore $0 = M_a^p - 1_V = (M_a - 1_V)^p$. $\square$

Let us now define an important V-subspace:

$$W(\mathcal{T}) \stackrel{\text{def}}{=} \{a \mid \sigma_a \in \mathcal{T}\} = \{a \mid \sigma_a = \tau_a\}.$$

We will sometimes denote $W(\mathcal{T})$ by $W_\circ$. It is easily checked that $W(\mathcal{T})$ is a subspace of $(V, +)$ and $(V, \circ)$. Such a subspace is nontrivial for the following theorem, proven in [16]. It is straightforward but important to notice that if $a \in W(\mathcal{T})$, then $x + a = x \circ a$ holds for each $x \in V$, and consequently $M_a = 1_n$.

Theorem 3.3 *([16]). Let $\mathcal{T} \leq \mathrm{AGL}(V, +)$ be an abelian regular subgroup. If V is finite, then $T \cap \mathcal{T} \neq \langle 1_V \rangle$.*

We will show soon that $W(\mathcal{T})$ plays an important role for the characterisation of maps in the group $\mathcal{T}$.

Our purpose is, given an operation $\circ$ induced by the group $\mathcal{T} = \{\tau_a \mid a \in V\}$, to describe the matrices M_a for each $a \in V$, where $\tau_a = M_a\sigma_a$. We show now some preliminary results.

Let U be a subspace of V. Then for all $\gamma \in \mathrm{GL}(V)$ such that $U\gamma = U$, the action of γ over V/U is well defined by means of the map $\bar{\gamma} : [v] \mapsto [v\gamma]$ in $\mathrm{GL}(V/U)$. Let us prove now the following characterisation, recalling that $\mathcal{U}(V)$ denotes the group of upper unitriangular linear maps.

Lemma 3.4. *Let $M_i \in \mathcal{U}(V)$ be a unitriangular map acting as the identity on the quotient $V/\mathrm{Span}\{e_{i+1}, \ldots, e_n\}$, for each $1 \leq i \leq n$. Then, the affine transformations $M_i\sigma_{e_i}$ generate a transitive subgroup of $\mathrm{AGL}(V)$.*

Proof. Denote by τ_{e_i} the transformation $M_i\sigma_{e_i}$. Let us start by observing that for each $1 \leq i \leq n$ the action of M_i over $V/\mathrm{Span}\{e_{i+1}, \dots, e_n\}$ is well defined and from the hypotheses τ_{e_i} acts on vectors of V leaving the first $i-1$ coordinates unchanged. Let now $v = (v^1, v^2, \dots, v^n)$ and $w = (w^1, w^2, \dots, w^n)$ be two elements of V and let us show that there exists $\tau \in \langle \tau_{e_1}, \tau_{e_2}, \dots, \tau_{e_n} \rangle$ such that $v\tau = w$. Let $\gamma^1 \in \mathbb{F}_p$ such that $v^1 + \gamma^1 = w^1$. So

$$v\,(\tau_{e_1})^{\gamma^1} = (w^1, v^2 + c^2, \dots, v^n + c^n) \stackrel{\text{def}}{=} v',$$

for some $c^i \in \mathbb{F}_p$ for $2 \leq i \leq n$, where c^i depends on v, τ_{e_1} and γ^1. Analogously, if $\gamma^2 \in \mathbb{F}_p$ is such that $(v')^2 + \gamma^2 = w^2$, then

$$v'\,(\tau_{e_2})^{\gamma^2} = (w^1, w^2, v^3 + d^3, \dots, v^n + d^n),$$

for some $d^i \in \mathbb{F}_p$ for $3 \leq i \leq n$. In this way, we obtain

$$\tau \stackrel{\text{def}}{=} (\tau_{e_1})^{\gamma^1}\,(\tau_{e_2})^{\gamma^2} \cdots (\tau_{e_n})^{\gamma^n}$$

such that $v\tau = w$, hence the transitivity is proven. $\square$

Remark 3.5. Notice that in the conditions of Lemma 3.4, if $\circ$ denotes the operation induced by $\mathcal{T} = \langle \tau_{e_1}, \tau_{e_2}, \dots, \tau_{e_n} \rangle$, then $\{e_i\}_{i=1}^n$ is a basis of $(V, \circ)$. However, this is not true in general. In the following example on $V = (\mathbb{F}_2)^3$ indeed, the canonical basis is not a basis for $(V, \circ)$. Let $T_\circ$ be defined in the following way:

$$T_\circ \stackrel{\text{def}}{=} \langle M_{(1,0,1)}\sigma_{(1,0,1)}, M_{(0,1,1)}\sigma_{(0,1,1)}, M_{(1,1,1)}\sigma_{(1,1,1)} \rangle,$$

where

$$M_{(1,0,1)} \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \; M_{(0,1,1)} \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \text{ and } M_{(1,1,1)} \stackrel{\text{def}}{=} 1_n.$$

Then the translations $\tau_{e_1}, \tau_{e_2}, \tau_{e_3}$ are respectively individuated by the matrices

$$M_{e_1} \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \; M_{e_2} \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix} \text{ and } M_{e_3} \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

It is a straightforward check that $e_1 \circ e_2 = e_3$.

Let us now show a more general result which will be useful later. The following well-known result (see e.g. [30, pag. 62]) is needed.

Theorem 3.6. *Let $H \leq \mathrm{GL}(V)$ be a group of unipotent matrices. Then there exists a basis of V in which all elements of H are upper triangular.*

Lemma 3.7. *Let $G < \mathrm{GL}(V)$ be a unipotent subgroup and let $U \subseteq V$ be a subspace such that for all $v \in U$ and $g \in G$ we have $vg = v$, i.e. G is a subgroup of the pointwise stabiliser of U. Let $d \stackrel{\text{def}}{=} \dim(U)$ and $m \stackrel{\text{def}}{=} n - d$. Then all elements of G are upper triangular in a basis $\{v_1, \dots, v_m, v_{m+1}, \dots, v_{m+d}\}$, where $\{v_{m+1}, \dots, v_{m+d}\}$ is any basis of U.*

Proof. Since G fixes all the elements of U, it acts as a group of unipotent maps on V/U. From Theorem 3.6 there exists a basis $[v_1], \dots, [v_m]$ of V/U, such that $[v_i]g - [v_i]$ lies in $\mathrm{Span}\{[v_{i+1}], \dots, [v_m]\}$ for all $g \in G$. Then, all elements of G are upper triangular in the basis $\{v_1, \dots, v_m, v_{m+1}, \dots, v_n\}$, since $v_i g - v_i = 0$ for all $m + 1 \le i \le n$. □

The previous result reads in the way displayed below, when specified to our case.

Corollary 3.8. *Let $\mathcal{T} < \mathrm{AGL}(V)$ be an elementary abelian regular group. Let $d \stackrel{\text{def}}{=} \dim(W(\mathcal{T}))$ and let $m \stackrel{\text{def}}{=} n - d$. Then all elements of $\Omega(\mathcal{T})$ are upper triangular in a basis $\{v_1, \dots, v_{m+1}, \dots, v_n\}$, where $\{v_{m+1}, \dots, v_n\}$ is any basis of $W(\mathcal{T})$.*

Proof. By Proposition 3.2, $\Omega(\mathcal{T})$ is unipotent. Moreover, by definition, for all $v \in W(\mathcal{T})$ and $M \in \Omega(\mathcal{T})$ we have $vM = v$. Hence, the claim follows from Lemma 3.7. □

The results obtained so far may be summarised in the following theorem. According to this result, when considering an operation $\circ$ we can always assume, up to conjugation, that $W_\circ$ is generated by the last vectors of the canonical basis.

Theorem 3.9. *Let $\mathcal{T} < \mathrm{AGL}(V)$ be an elementary abelian regular group. Let $d \stackrel{\text{def}}{=} \dim(W(\mathcal{T}))$ and let $m \stackrel{\text{def}}{=} n - d$. Then there exists $g \in \mathrm{GL}(V)$ such that $\Omega(\mathcal{T}^g) < \mathcal{U}(V)$ and $W(\mathcal{T}^g) = \mathrm{Span}\{e_{m+1}, \dots, e_n\}$.*

Proof. From Corollary 3.8, all the elements of $\Omega(\mathcal{T})$ are upper triangular with respect to a basis $\{v_1, \dots, v_n\}$ of V, whose last d vector form a basis of $W(\mathcal{T})$. Let $g \in \mathrm{GL}(V)$ such that $v_i g = e_i$ for each $1 \le i \le n$. It is easy to check that $\Omega(\mathcal{T}^g) = \Omega(\mathcal{T})^g$, then for all $M \in \Omega(\mathcal{T})$ we have

$$e_i g^{-1} M g - e_i = v_i M g - v_i g = (v_i M - v_i) g.$$

Since $v_i M - v_i \in \mathrm{Span}\{v_{i+1}, ..., v_n\}$, we have $(v_i M - v_i) g \in \mathrm{Span}\{e_{i+1}, ..., e_n\}$. In conclusion, from $(\tau_v)^g : x \mapsto x\,(M_v)^g\, g + vg$, we also obtain $W(\mathcal{T}^g) = W(\mathcal{T}) g = \mathrm{Span}\{e_{m+1}, \dots, e_n\}$. □

Till now we have assumed that the subgroup $\mathcal{T}$ is an affine group. For reasons already explained in Sec. 2 and related to the application in cryptography of this construction, we are interested in groups whose normalisers contain the group of translations T_+, i.e. in operations $T_\circ$ for which, given $g \in \mathrm{Sym}(V)$ such that $\mathcal{T} = T_+^g$, we also have

$T_+ < \mathrm{AGL}(V, \circ) = \mathrm{AGL}(V, +)^g$. Let us report a result from [16] which is useful for our purpose.

Lemma 3.10. *Let $\mathcal{T} < \mathrm{AGL}(V)$ be abelian and regular. Then for each $\sigma_x \in T_+$ and $\tau_y \in \mathcal{T}$ we have*

$$[\sigma_x, \tau_y] = \sigma_{x \cdot y},$$

where $\cdot$ denotes the product of the $\mathbb{F}_p$-algebra related to $\mathcal{T}$ as in Theorem 3.1, and $[\sigma_x, \tau_y] \stackrel{\text{def}}{=} \sigma_x^{-1}\tau_y^{-1}\sigma_x\tau_y$.

In our case, from Lemma 3.10 we obtain that T normalises $\mathcal{T} < \mathrm{AGL}(V)$ if and only if $\sigma_{x \cdot y} \in \mathcal{T}$ for all $x, y \in V$. Indeed, if for all $\sigma_x \in T$ we have $\mathcal{T}^{\sigma_x} = \mathcal{T}$, then

$$\sigma_{x \cdot y} = \sigma_x^{-1}\tau_y^{-1}\sigma_x\tau_y \in \mathcal{T}.$$

Conversely, if $\sigma_{x \cdot y} \in \mathcal{T}$ for each $x, y \in V$, then

$$\mathcal{T} \ni \sigma_{x \cdot y}\tau_y^{-1} = \sigma_x^{-1}\tau_y^{-1}\sigma_x.$$

Finally notice that the condition $\sigma_{x \cdot y} \in \mathcal{T}$ for all $x, y \in V$ is equivalent to $x \cdot y \cdot z = 0$ for all $x, y, z \in V$.

We are now ready to prove one of the main results of this work, i.e. the structure of affine translation groups whose normalisers contain the group T_+. Before doing so, let us recall that for sake of simplicity, proceeding as in Sec. 2, given a group $\mathcal{T} = T_\circ < \mathrm{AGL}(V)$, we denote by $\mathrm{AGL}(V, \circ)$ the normaliser in $\mathrm{Sym}(V)$ of $\mathcal{T}$, which is $\mathrm{AGL}(V, +)^g$ where $g \in \mathrm{Sym}(V)$ is such that $\mathcal{T} = T^g$.

Theorem 3.11. *Let $\mathcal{T} < \mathrm{AGL}(V, +)$ be elementary abelian regular and let $\circ$ be the operation induced on V. Let $d \stackrel{\text{def}}{=} \dim(W(\mathcal{T}))$, let $m \stackrel{\text{def}}{=} n - d$ and let us assume $W(\mathcal{T}) = \mathrm{Span}\{e_{m+1}, \dots, e_n\}$. Then, $T_+ < \mathrm{AGL}(V, \circ)$ if and only if for all $M_y \in \Omega(\mathcal{T})$ there exists a matrix $B_y \in (\mathbb{F}_p)^{m \times d}$ such that*

$$M_y = \begin{pmatrix} 1_m & B_y \\ 0 & 1_d \end{pmatrix}. \tag{2}$$

Proof. By Theorem 3.9, there exists another group operation $\diamond$ on V such that the corresponding translation group is conjugated, by an element of $\mathrm{GL}(V)$, to $T_\circ$ and satisfies $W(T_\diamond) = W(T_\circ)$ and $\Omega(T_\diamond) = \{\overline{M_a} \mid a \in V\} < \mathcal{U}(V)$. Let $y \in V$ and let $A_y \in (\mathbb{F}_p)^{m \times m}$ an upper-triangular matrix and $B_y \in (\mathbb{F}_p)^{m \times d}$ such that

$$\overline{M_y} = \begin{pmatrix} A_y & B_y \\ 0 & 1_d \end{pmatrix}.$$

Notice that the lower structure of the matrix derives by the property $e_i \in W(T_\diamond)$ for each $m+1 \leq i \leq n$, i.e. $y \diamond e_i = e_i\overline{M}_y + y = y + e_i$ for each $m+1 \leq i \leq n$. Recall that

$$T_+ < \mathrm{AGL}(V, \diamond) \iff \forall x, y \in V \quad x \cdot y \in W(T_\diamond) \tag{3}$$

$$\iff \forall x, y \in V \quad x\overline{M_y} - x \in W(T_\diamond), \tag{4}$$

where the equivalence in Eq. (3) derives from Lemma 3.10. From Eq. (4) instead, considering $x \in \mathrm{Span}\{e_1, \ldots, e_m\}$ we obtain that $x\overline{M_y} - x \in W(T_\diamond)$ if and only if $A_y = 1_m$.

In order to conclude, we need to prove that each conjugate $T_\circ = {T_\diamond}^g$ is such that all the matrices in the group $\Omega(T_\circ)$ are as in Eq. (2), provided that $g \in \mathrm{GL}(V)$ and $W(T_\circ)$ is spanned by the last d vectors of the canonical basis. Let $g \in \mathrm{GL}(V)$ such that $T_\circ = T_\diamond^g$. Since $W(T_\diamond)g = W({T_\diamond}^g) = W(T_\circ)$, then $\mathrm{Span}\{e_{m+1}, \ldots, e_n\}g = \mathrm{Span}\{e_{m+1}, \ldots, e_n\}$ and also $\mathrm{Span}\{e_{m+1}, \ldots, e_n\}g^{-1} = \mathrm{Span}\{e_{m+1}, \ldots, e_n\}$. Consequently

$$g = \begin{pmatrix} G_1 & G_2 \\ 0 & G_3 \end{pmatrix} \text{ and } g^{-1} = \begin{pmatrix} G_1^{-1} & {G_2}' \\ 0 & G_3^{-1} \end{pmatrix},$$

for some $G_1 \in (\mathbb{F}_p)^{m\times m}, G_2, {G_2}' \in (\mathbb{F}_p)^{m\times d}$ and $G_3 \in (\mathbb{F}_p)^{d\times d}$. Thus, if $M \in \Omega(T_\diamond)$ we have

$$M^g = \begin{pmatrix} G_1^{-1} & {G_2}' \\ 0 & G_3^{-1} \end{pmatrix} \begin{pmatrix} 1_m & B_{m\times d} \\ 0 & 1_d \end{pmatrix} \begin{pmatrix} G_1 & G_2 \\ 0 & G_3 \end{pmatrix} = \begin{pmatrix} 1_m & {B'}_{m\times d} \\ 0 & 1_d \end{pmatrix},$$

therefore the claim follows from $\Omega(T_\circ) = \Omega({T_\diamond}^g) = \Omega(T_\diamond)^g$. $\square$

The characterisation given above allows to construct an isomorphism between the vector spaces $(V, \circ)$ and $(V, +)$, which can be computed very efficiently (see [14]). This makes some attacks feasible [14,20]. Moreover, Theorem 3.11 can be used to determine the maps contained in $\mathrm{GL}(V, \circ) \cap \mathrm{GL}(V, +)$ (see [13,20]).

4. Even characteristic and combinatorial formulas

In this section we specialise our focus to the cryptographically-relevant case of binary fields. Let us assume from now on that $p = 2$. In this case, we can prove (see Theorem 4.1 and Theorem 4.7) an upper bound on the number of the elementary abelian regular subgroups as in Theorem 3.11. Moreover, we can calculate the number of these groups if the co-dimension of $W(T_\circ)$ is 2 or 3. To conclude, we report the full classification of the elementary abelian regular subgroups of $\mathrm{AGL}(V, +)$ up to dimension 6. Before doing so, let us prove the following result which bounds the dimension of the subspace $W(T_\circ)$.

Proposition 4.1. *Let $\mathcal{T} < \mathrm{AGL}(V, +)$ be elementary abelian regular and let $d \stackrel{\text{def}}{=} \dim(W(\mathcal{T}))$. If $\mathcal{T} \neq T$, then*

$$\frac{(-1)^n + 3}{2} \leq d \leq n - 2.$$

Proof. From Theorem 3.3 and from the hypothesis we have $1 \leq d \leq n-1$. Let us now assume that $W(\mathcal{T})$ contains $n-1$ linearly independent vectors $v_1, v_2 \ldots, v_{n-1} \in V$ and let $v_n \in V$ independent from $v_1, \ldots, v_{n-1}$. Let $\circ$ be the operation induced by $\mathcal{T}$. Then, $v_i \circ v_n = v_i + v_n$, thus $v_i M_{v_n} = v_i$ for all $1 \leq i \leq n-1$. Moreover, $v_n \circ v_n = 0$ and so $v_n M_{v_n} = v_n$. Then, if $v \in V$, then

$$v \circ v_n = \left(\sum_{i<n} \xi_i v_i + \xi_n v_n \right) M_{v_n} + v_n = \sum_{i<n} \alpha_i v_i + \alpha_n v_n + v_n = v + v_n,$$

which implies $d = n$, a contradiction. If n is even, then $d > 1$, i.e. $T \cap \mathcal{T}$ contains at least four elements. A proof of this fact may be found in [13]. □

Let us now prove that if $\mathcal{T}$ normalises T and the co-dimension of $W(\mathcal{T})$ is at most 5, then we also have that T normalises $\mathcal{T}$.

Proposition 4.2. *Let $\mathcal{T} < \mathrm{AGL}(V)$ be elementary abelian regular, and let $\circ$ be the operation induced. Let $d \overset{\text{def}}{=} \dim(W(\mathcal{T}))$ and $m \overset{\text{def}}{=} n - d$. If $2 \leq m \leq 5$, then $\mathrm{AGL}(V, \circ)$ contains T.*

Proof. The claim follows if we prove that if $x, y \in V$, then $x \cdot y \in W(\mathcal{T})$. Let $x, y \in V$ and let us assume by contradiction $x \cdot y \notin W(\mathcal{T})$. Then there exists $z \notin W(\mathcal{T})$ such that $x \cdot y \cdot z \neq 0$. Let us show that $x, y, z, x \cdot y, x \cdot z, y \cdot z, x \cdot y \cdot z$ are linearly independent. Let $\xi_i \in \mathbb{F}_2$ for $1 \leq i \leq 7$ such that

$$\xi_1 x + \xi_2 y + \xi_3 z + \xi_4 x \cdot y + \xi_5 x \cdot z + \xi_6 y \cdot y + \xi_7 x \cdot y \cdot z = 0.$$

By multiplying each member of the previous equation by $y \cdot z$ we obtain $\xi_1 x \cdot y \cdot z = 0$, which implies $\xi_1 = 0$. In the same way, by multiplying by $x \cdot z$ we prove $\xi_2 = 0$. Proceeding in this way one proves that $\xi_i = 0$ for each $1 \leq i \leq 7$. This proves that $x, y, z, x \cdot y, x \cdot z, y \cdot z, x \cdot y \cdot z$ are linearly independent and none of these belongs to $W(\mathcal{T})$. Using a similar argument one proves that $\mathrm{Span}\{x, y, z, x \cdot y, x \cdot z, y \cdot z, x \cdot y \cdot z\} \cap W(\mathcal{T}) = \{0\}$. This implies $m \geq 6$, a contradiction. □

We have presented the previous result in the way which best fit our needs. However, it can be stated more generally in the following way.

Proposition 4.3. *Let $\mathcal{T}_1, \mathcal{T}_2 < \mathrm{Sym}(V)$ be elementary abelian regular. Let d be such that $2^d = |\mathcal{T}_1 \cap \mathcal{T}_2|$, $m \overset{\text{def}}{=} n - d$ and let us assume $2 \leq m \leq 5$. Then $\mathcal{T}_1$ is contained in the normaliser of $\mathcal{T}_2$ if and only if $\mathcal{T}_2$ is contained in the normaliser of $\mathcal{T}_1$.*

Example 4.4. Notice that Proposition 4.2 does not hold, in general, for $m \geq 6$. Let $(V, +, \cdot)$ be the exterior algebra over a vector space of dimension three, spanned by e_1, e_2, e_3. Hence a basis of V is composed by

$$e_1, e_2, e_3, e_4 = e_1 \wedge e_2, e_5 = e_1 \wedge e_3, e_6 = e_2 \wedge e_3, e_7 = e_1 \wedge e_2 \wedge e_3.$$

The associated translation group $T_\circ$ is such that $W(T_\circ) = \mathrm{Span}\{e_7\}$, but we have

$$M_{e_1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & \boxed{1} & 0 & 0 & 0 \\ & & 1 & 0 & \boxed{1} & 0 & 0 \\ & & & 1 & 0 & 0 & 0 \\ & & & & 1 & 0 & 0 \\ & & & & & 1 & 1 \\ & & & & & & 1 \end{pmatrix}.$$

From Theorem 3.11, $\mathrm{AGL}(V, \circ)$ cannot contain the group T_+.

Let us now point out, starting from Theorem 3.11, some properties of the matrices in $\Omega(T_\circ)$ defining the operation $\circ$. Let us assume $T_\circ < \mathrm{AGL}(V)$ be elementary abelian regular and let us denote, as usual, $d \stackrel{\text{def}}{=} \dim(W(T_\circ))$ and $m \stackrel{\text{def}}{=} n - d$. Let $1 \leq i \neq j \leq m$. Since $e_i \circ e_i = e_i M_{e_i} + e_i = 0$ we obtain that the i-th row of B_{e_i} is zero, where

$$M_{e_i} = \begin{pmatrix} 1_m & B_{e_i} \\ 0 & 1_d \end{pmatrix}.$$

Instead, from $e_i \circ e_j = e_i M_{e_j} + e_j = e_j M_{e_i} + e_i = e_j \circ e_i$, we obtain that the j-th row of B_{e_i} equals the i-th row of B_{e_j}. Moreover, let $x \in V$. Then

$$\begin{aligned} x \circ e_i \circ e_j &= (x M_{e_i} + e_i) \circ e_j \\ &= (x M_{e_i} + e_i) M_{e_j} + e_j \\ &= x M_{e_i} M_{e_j} + e_i M_{e_j} + e_j \\ &= x M_{e_i} M_{e_j} + e_i \circ e_j, \end{aligned}$$

which proves that $M_{e_i \circ e_j} = M_{e_i} M_{e_j}$, i.e.

$$M_{e_i \circ e_j} = \begin{pmatrix} 1_m & B_{e_i} + B_{e_j} \\ 0 & 1_d \end{pmatrix}.$$

This fact is easily generalised as follows.

Proposition 4.5. *Let $T_\circ < \mathrm{AGL}(V)$ be an elementary abelian regular group. Let $d \stackrel{\text{def}}{=} \dim(W(T_\circ))$ and $m \stackrel{\text{def}}{=} n - d$. Moreover, let us assume $W(T_\circ) = \mathrm{Span}\{e_{m+1}, \ldots, e_n\}$ and $T < \mathrm{AGL}(V, \circ)$. Let $x \in V$, $x = \xi_1 e_1 \circ \cdots \circ \xi_n e_n$ for some $\xi_i \in \mathbb{F}_2$. Then*

$$M_x = \begin{pmatrix} 1_m & \sum_{i=1}^{m} \xi_i B_{e_i} \\ 0 & 1_d \end{pmatrix}.$$

Proof. From the hypothesis we have that the canonical basis of $(V, +)$ is a basis also for $(V, \circ)$ (see Remark 3.5). Moreover, $B_{e_i} \neq 0$ for $1 \leq i \leq m$ and $B_{e_i} = 0$ for $m \leq i \leq n$. The claim follows straightforwardly by writing x in terms of e_is in $(V, \circ)$. □

4.1. Some combinatorial results

In this section we will examine some combinatorial aspects of our topic, focusing on counting the number of abelian regular subgroups of the affine group which are useful in cryptographic contexts. In the next result we will count them in terms of points of a given geometric variety. Let $T_\circ$ be as in Proposition 4.5. For each $1 \leq i \leq m$ we will denote the entries in the matrix M_{e_i} in the following way:

$$M_{e_i} = \begin{pmatrix} & b_{1,1}^{(i)} & \dots & b_{1,d}^{(i)} \\ 1_m & \vdots & & \vdots \\ & b_{m,1}^{(i)} & \dots & b_{m,d}^{(i)} \\ \\ 0 & & 1_d & \\ \\ \end{pmatrix}. \tag{5}$$

In what follows, in order to keep the notation more compact, given a positive integer s we will denote by $[s]$ the set $\{1, \dots, s\}$.

Theorem 4.6. *Let $d \geq 1$. The number of elementary abelian regular subgroups $T_\circ < \mathrm{AGL}(V, +)$ such that $\dim(W(T_\circ)) = d$ and $T_+ < \mathrm{AGL}(V, \circ)$ is*

$$\begin{bmatrix} n \\ d \end{bmatrix}_2 \cdot |\mathcal{V}(\mathcal{I}_{m,d})|, \tag{6}$$

where $m = n - d$, $\mathcal{I}_{m,d}$ is the ideal in $\mathbb{F}_2\left[b_{i,j}^{(s)} \middle| i, s \in [m],\ j \in [d]\right]$ generated by $\mathcal{S}_0 \cup \mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3$ with

$$\mathcal{S}_0 \stackrel{\text{def}}{=} \left\{ \left(b_{i,j}^{(s)}\right)^2 - b_{i,j}^{(s)} \middle| i, s \in [m], j \in [d] \right\},$$

$$\mathcal{S}_1 \stackrel{\text{def}}{=} \left\{ \prod_{i=1}^{m} \prod_{j=1}^{d} \left(1 + \sum_{s \in S} b_{i,j}^{(s)}\right) \middle| S \subseteq [m], S \neq \emptyset \right\},$$

$$\mathcal{S}_2 \stackrel{\text{def}}{=} \left\{ b_{i,j}^{(s)} - b_{s,j}^{(i)} \middle| i, s \in [m], j \in [d] \right\},$$

$$\mathcal{S}_3 \stackrel{\text{def}}{=} \left\{ b_{i,j}^{(i)} \middle| i \in [m], j \in [d] \right\},$$

$\mathcal{V}(\mathcal{I}_{m,d})$ is the variety of $\mathcal{I}_{m,d}$ and $\begin{bmatrix} n \\ d \end{bmatrix}_2 \stackrel{\text{def}}{=} \prod_{i=0}^{d-1} \frac{2^{n-i}-1}{2^{d-i}-1}$ *is the Gaussian binomial.*

Proof. The claim follows by applying together Theorem 3.11 and Theorem 3.9. Let us start by computing the number of the groups as in Theorem 3.11, and then all the conjugates one can obtain from these. Notice that a group $T_\circ < \mathrm{AGL}(V,+)$ such that $W(T_\circ)$ is generated by the last d vectors of the canonical basis of V and such that $T_+ < \mathrm{AGL}(V,\circ)$ is determined if the matrices $M_{e_1},\dots,M_{e_m}$ (and so, equivalently, $B_{e_1},\dots,B_{e_m}$) are individuated, since $M_{e_i} = 1_n$ for the remaining $m < i \le n$. We will show that to each set of admissible matrices $\{B_{e_1},\dots,B_{e_m}\}$ corresponds one point in $\mathcal{V}(\mathcal{I}_{m,d})$ and vice versa, from a point of $\mathcal{V}(\mathcal{I}_{m,d})$ we can obtain one set of admissible matrices $\{B_{e_1},\dots,B_{e_m}\}$. Let $T_\circ < \mathrm{AGL}(V,+)$ be such that $W(T_\circ)$ is generated by the last d vectors of the canonical basis of V and such that $T_+ < \mathrm{AGL}(V,\circ)$. Let us denote by $\{M_{e_1},\dots,M_{e_m}\}$ the matrices defining the operation. If $\emptyset \neq S \subseteq [m]$ and $x = \bigcirc_{i\in S} e_i$, then, from Proposition 4.5,

$$M_x = \begin{pmatrix} & \sum_{s\in S} b_{1,1}^{(s)} & \dots & \sum_{s\in S} b_{1,d}^{(s)} \\ 1_m & \vdots & & \vdots \\ & \sum_{s\in S} b_{m,1}^{(s)} & \dots & \sum_{s\in S} b_{m,d}^{(s)} \\ 0 & & 1_d & \end{pmatrix}.$$

Since $M_x \neq 1_V$, then there exist i,j such that

$$\sum_{s\in S} b_{i,j}^{(s)} = 1,$$

which happens if and only if

$$\prod_{i=1}^{m}\prod_{j=1}^{d}\left(1 + \sum_{s\in S} b_{i,j}^{(s)}\right) = 0.$$

For symmetry we also have that the conditions given by set $\mathcal{S}_2$ hold. Moreover, since e_i is fixed from M_{e_i}, we also obtain a solution for set $\mathcal{S}_3$. To conclude, $\mathcal{S}_0$ is trivially satisfied, since the matrices are binary.

Vice versa, from a solution of the ideal $\mathcal{I}_{m,d}$, we can construct $B_{e_1}, \dots, B_{e_m}$ as in Eq. (5). Consequently, we can consider the group $\mathcal{T}$ generated by the affine maps $\tau_{e_i} \stackrel{\text{def}}{=} M_{e_i}\sigma_{e_i}$ for $1 \le i \le n$, where for $1 \le i \le m$

$$M_{e_i} \stackrel{\text{def}}{=} \begin{pmatrix} 1_m & B_{e_i} \\ 0 & 1_d \end{pmatrix}$$

and $M_{e_i} \stackrel{\text{def}}{=} 1_n$ for $m < i \le n$. Since the conditions of Lemma 3.4 are satisfied, $\mathcal{T}$ is transitive, and it is abelian from the condition expressed by set $\mathcal{S}_2$. Moreover, if $x \in V$ and $1 \le i \le m$, then

$$x\tau_{e_i}^2 = (xM_{e_i}^2 + e_i M_{e_i} + e_i).$$

Computing $M_{e_i}^2$ we obtain

$$M_{e_i}^2 = \begin{pmatrix} 1_m & B_{e_i} + B_{e_i} \\ 0 & 1_d \end{pmatrix} = 1_n.$$

Hence, since from the condition given by set $\mathcal{S}_3$ we obtain $e_i M_{e_i} = e_i$, and so $\tau_{e_i}^2 = 1_V$, i.e. $\mathcal{T}$ is elementary. Moreover, $\mathcal{T}$ is regular, since it is abelian and transitive.

This shows a one-to-one correspondence between the points of $\mathcal{V}(\mathcal{I}_{m,d})$ and the subgroups $T_\circ < \mathrm{AGL}(V,+)$ such that $W(T_\circ) = \mathrm{Span}\{e_{m+1}, \dots, e_n\}$ and $T_+ < \mathrm{AGL}(V,\circ)$. To conclude, consider a d-dimensional vector subspace $\overline{W} < V$ and let $\Delta = |\mathcal{V}(\mathcal{I}_{m,d})|$. Let us denote by $\mathcal{T}_1, \dots, \mathcal{T}_\Delta$ the distinct elementary abelian regular groups such that $W(\mathcal{T}_i) = \mathrm{Span}\{e_{m+1}, \dots, e_n\}$ and let $g \in \mathrm{GL}(V,+)$ be a transformation such that $\overline{W}g = \mathrm{Span}\{e_{m+1}, \dots, e_n\}$. Then the groups $(\mathcal{T}_1)^{g^{-1}}, \dots, (\mathcal{T}_\Delta)^{g^{-1}}$ are pairwise distinct and $W((\mathcal{T}_i)^{g^{-1}}) = \overline{W}$ for each $1 \le i \le \Delta$. Now, let $T_\diamond$ be an elementary abelian regular subgroup such that $W(T_\diamond) = \overline{W}$. We have $W((T_\diamond)^g) = W(T_\diamond)g = \mathrm{Span}\{e_{m+1}, \dots, e_n\}$, which implies $(T_\diamond)^g = \mathcal{T}_i$ for some i, and so $T_\diamond = (\mathcal{T}_i)^{g^{-1}}$. Our claim follows from the fact that the number of d-dimensional vector subspaces of an n-dimensional vector space over $\mathbb{F}_2$ is $\begin{bmatrix} n \\ d \end{bmatrix}_2$. $\square$

In the next result, we give an upper bound on the number of points of the variety $\mathcal{V}(\mathcal{I}_{m,d})$ defined in Theorem 4.6. A lower bound to $|\mathcal{V}(\mathcal{I}_{m,d})|$ has been given in [13], where it is also shown that the upper bound of Theorem 4.7 is tight.

Theorem 4.7. *Let $\mathcal{I}_{m,d}$ be defined as in Theorem 4.6. Then*

$$|\mathcal{V}(\mathcal{I}_{m,d})| \le 2^{d\frac{m(m-1)}{2}} - 1 - \sum_{r=1}^{m-2} \binom{m}{r} \left(2^d - 1\right)^{\binom{m-r}{2}}.$$

Proof. Let $\overline{B} = (b_1^{(1)}, \dots, b_m^{(1)}, b_1^{(2)}, \dots, b_m^{(2)}, \dots, b_1^{(m)}, \dots, b_m^{(m)}) \in \mathcal{V}(\mathcal{I}_{m,d})$, where $b_i^{(s)} = (b_{i,1}^{(s)}, \dots b_{i,d}^{(s)}) \in (\mathbb{F}_2)^d$ for all i, j as in (5), i.e. $b_i^{(s)}$ is the i-th row of the matrix B_{e_s}.

We aim at counting how many vectors $\overline{B}$ satisfy the constrains of set $\mathcal{S}_1$, $\mathcal{S}_2$ and $\mathcal{S}_3$ as in Theorem 4.6. We proceed in two steps: we consider first all the solutions for $\mathcal{S}_2$ and $\mathcal{S}_3$ and then we exclude some of those for which the equations of $\mathcal{S}_1$ are not satisfied.

First step. As already pointed out before Proposition 4.5, from the conditions in $\mathcal{S}_3$ we have $b_i^{(i)} = 0$ for all i, and from those in $\mathcal{S}_2$, $b_j^{(i)} = b_i^{(j)}$ for all i, j. Therefore, the matrix B_{e_1} is determined only by the rows $b_2^{(1)}, \dots, b_m^{(1)}$, being its first row equal to zero. Analogously, B_{e_2} is determined only by the rows $b_3^{(2)}, \dots, b_m^{(2)}$ and by $b_2^{(1)}$, since the first row of B_{e_2} is equal to the second row of B_{e_1} and since the second row of B_{e_2} equal to zero. Iterating this argument we can consider only the vector composed as

$$B = (\underbrace{b_2^{(1)}, \dots, b_m^{(1)}}, \underbrace{b_3^{(2)}, \dots, b_m^{(2)}}, \dots, \underbrace{b_{m-1}^{(m-2)}, b_m^{(m-2)}}, \underbrace{b_m^{(m-1)}})$$

and thus we have $2^{d\frac{m(m-1)}{2}}$ solutions to the equations in $\mathcal{S}_2 \cup \mathcal{S}_3$.

Second step. The entries of B must satisfy also the constrains given by $\mathcal{S}_1$, so for any subset $S \subset [m]$ we can exclude the cases where

$$\begin{cases} B_{e_i} = 0 & \text{if } i \in S \\ B_{e_i} \neq 0 & \text{if } i \notin S. \end{cases}$$

In particular, we count when the entries of the matrices B_{e_i} with $i \in S$ are all zeros and the remaining entries of the matrices B_{e_i} with $i \notin S$ are all non-zero. We start considering those vectors B obtained when exactly one B_{e_i} is zero and others are non-zero, that is, we consider any set S with one element. In this case $n-1$ entries of B are zero and the others are all non-zero. Similarly, if any pair (B_{e_s}, B_{e_t}) is equal to zero and the others are not, then $m-1+m-2$ entries of B are zero and the others are all non-zero. Indeed, assuming $s < t$, the zero entries of B must be $b_s^{(1)}, ..., b_s^{(s-1)}, b_{s+1}^{(s)}, ..., b_m^{(s)}$ in order to have $B_{e_s} = 0$, and $b_t^{(1)}, ..., b_t^{(t-1)}, b_{t+1}^{(t)}, ..., b_m^{(t)}$ in order to have $B_{e_t} = 0$. Considering that $b_t^{(s)}$ is already zero, we have that $m-1+m-2$ entries of B are zero. Iterating this argument, if we assume that r matrices are zero, then $\sum_{i=1}^{r}(m-i)$ entries of B are zero and the others are all non-zero. Then such r matrices can be chosen in $\binom{m}{r}$ possible ways and any time $2^d - 1$ non-zero elements may be used to fill each of the other entries of B, that are

$$\begin{aligned} \frac{m(m-1)}{2} - \sum_{i=1}^{r}(m-i) &= \binom{m}{2} - \sum_{i=m-r}^{m-1} i \\ &= \binom{m}{2} - \sum_{i=1}^{m-1} i + \sum_{i=1}^{m-r-1} i \end{aligned}$$

$$= \binom{m}{2} - \binom{m}{2} + \binom{m-r}{2}$$
$$= \binom{m-r}{2}.$$

The last case is when $m-1$ matrices B_{e_i} are zero. By the conditions of $\mathcal{S}_2 \cup \mathcal{S}_3$ also the last one is zero, and this happens only when B is zero. This concludes the proof. □

The following results are derived from Theorem 4.6 and are related to the special cases when $\dim(W(T_\circ)) \in \{n-3, n-2\}$. Notice that the case $\dim(W(T_\circ)) = n-2$ has been largely considered in [20], where it has been used to perform a differential attack against a block cipher. The same notation as in Theorem 4.6 is used. Recall that if $\mathcal{T} = T_\circ$, from Proposition 4.2, the hypothesis $T_\circ < \mathrm{AGL}(V, +)$ is enough to guarantee that $T_+ < \mathrm{AGL}(V, \circ)$, and so also Theorem 3.11 applies.

Corollary 4.8. *There exist*

$$\begin{bmatrix} n \\ n-3 \end{bmatrix}_2 \cdot \left(2^{3(n-3)} - 7(2^{n-3}-1) - 1\right)$$

distinct elementary abelian regular groups $\mathcal{T} < \mathrm{AGL}(V)$ *such that* $\dim(W(\mathcal{T})) = n-3$.

Proof. Proceeding as in Theorem 4.6, we need to compute the number of groups $\mathcal{T}$ such that $W(\mathcal{T}) = \mathrm{Span}\{e_4, \dots, e_n\}$. Using the notation as in Theorem 4.7, we have

$$M_{e_1} = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ & 1 & 0 & b_2^{(1)} \\ & & 1 & b_3^{(1)} \\ \hline & & & 1_{n-3} \end{array}\right), \qquad M_{e_2} = \left(\begin{array}{ccc|c} 1 & 0 & 0 & b_2^{(1)} \\ & 1 & 0 & 0 \\ & & 1 & b_3^{(2)} \\ \hline & & & 1_{n-3} \end{array}\right)$$

$$M_{e_3} = \left(\begin{array}{ccc|c} 1 & 0 & 0 & b_3^{(1)} \\ & 1 & 0 & b_3^{(2)} \\ & & 1 & 0 \\ \hline & & & 1_{n-3} \end{array}\right), \quad M_{e_1}M_{e_2} = \left(\begin{array}{ccc|c} 1 & 0 & 0 & b_2^{(1)} \\ & 1 & 0 & b_2^{(1)} \\ & & 1 & b_3^{(1)} + b_3^{(2)} \\ \hline & & & 1_{n-3} \end{array}\right)$$

$$M_{e_1}M_{e_3} = \left(\begin{array}{ccc|c} 1 & 0 & 0 & b_3^{(1)} \\ & 1 & 0 & b_2^{(1)} + b_3^{(2)} \\ & & 1 & b_3^{(1)} \\ \hline & & & 1_{n-3} \end{array}\right), \quad M_{e_2}M_{e_3} = \left(\begin{array}{ccc|c} 1 & 0 & 0 & b_2^{(1)} + b_3^{(1)} \\ & 1 & 0 & b_3^{(2)} \\ & & 1 & b_3^{(2)} \\ \hline & & & 1_{n-3} \end{array}\right)$$

$$M_{e_1}M_{e_2}M_{e_3} = \left(\begin{array}{ccc|c} 1 & 0 & 0 & b_2^{(1)} + b_3^{(1)} \\ & 1 & 0 & b_2^{(1)} + b_3^{(2)} \\ & & 1 & b_3^{(1)} + b_3^{(2)} \\ \hline & & & 1_{n-3} \end{array}\right).$$

The following possibilities need to be ruled out:

1. $M_{e_1} = 1_n \Leftrightarrow b_2^{(1)} = 0$ and $b_3^{(1)} = 0$,
2. $M_{e_2} = 1_n \Leftrightarrow b_2^{(1)} = 0$ and $b_3^{(2)} = 0$,
3. $M_{e_3} = 1_n \Leftrightarrow b_3^{(1)} = 0$ and $b_3^{(2)} = 0$,
4. $M_{e_1}M_{e_2} = 1_n \Leftrightarrow b_2^{(1)} = 0$ and $b_3^{(1)} = b_3^{(2)}$,
5. $M_{e_1}M_{e_3} = 1_n \Leftrightarrow b_3^{(1)} = 0$ and $b_2^{(1)} = b_3^{(2)}$,
6. $M_{e_2}M_{e_3} = 1_n \Leftrightarrow b_2^{(1)} = b_3^{(1)}$ and $b_3^{(2)} = 0$,
7. $M_{e_1}M_{e_2}M_{e_3} = 1_n \Leftrightarrow b_2^{(1)} = b_3^{(1)}$, $b_2^{(1)} = b_3^{(2)}$ and $b_3^{(1)} = b_3^{(2)}$.

Therefore we obtain that $2^{3(n-3)} - 7(2^{n-3} - 1) - 1$ is the number of distinct subgroups $\mathcal{T}$ such that $W(\mathcal{T}) = \mathrm{Span}\{e_4, \dots, e_n\}$. □

Corollary 4.9. *There exist*

$$\begin{bmatrix} n \\ n-2 \end{bmatrix}_2 \cdot (2^{n-2} - 1)$$

distinct elementary abelian regular groups $\mathcal{T} < \mathrm{AGL}(V)$ *such that* $\dim(W(\mathcal{T})) = n - 2$.

Proof. The proof is obtained using the same argument as in Corollary 4.8. □

Let us now prove that the groups of Corollary 4.9 belong to the same conjugacy class under $\mathrm{GL}(V)$.

Proposition 4.10. *Let* $\mathcal{T}$ *and* $\mathcal{T}'$ *elementary abelian regular subgroups of* $\mathrm{AGL}(V, +)$ *such that* $\dim(W(\mathcal{T})) = \dim(W(\mathcal{T}')) = n - 2$. *Then, there exists* $g \in \mathrm{GL}(V)$ *such that* $\mathcal{T}' = \mathcal{T}^g$.

Proof. It is enough to prove the claim for $\mathcal{T}$ and $\mathcal{T}'$ elementary abelian regular subgroups of $\mathrm{AGL}(V, +)$ such that $W(\mathcal{T}) = W(\mathcal{T}') = \mathrm{Span}\{e_3, \dots, e_n\}$. Recall that such groups are defined by the corresponding $(n-2)$-dimensional vectors, as shown in the proof of Theorem 4.7. Let us denote $\mathcal{T} = \langle \tau_{e_1}, \dots, \tau_{e_n} \rangle$ and $\mathcal{T}' = \langle \tau'_{e_1}, \dots, \tau'_{e_n} \rangle$, whose matrices are respectively individuated by the vectors

$$B = \left(b_{2,1}^{(1)}, \dots, b_{2,n-2}^{(1)}\right) \text{ and } B' = \left(b_{2,1}'^{(1)}, \dots, b_{2,n-2}'^{(1)}\right).$$

Let us assume first that B and B' have the same Hamming weight, i.e. the same number of non-zero coordinates. In this case there exists a permutation matrix $P \in$

$(\mathbb{F}_2)^{(n-2)\times(n-2)}$ such that $BP = B'$. Let $P' \in (\mathbb{F}_2)^{n\times n}$ be the permutation matrix defined as

$$P' \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & & & \\ \vdots & \vdots & & P & \\ 0 & 0 & & & \end{pmatrix}.$$

Note that when we multiply a matrix M by P' on the right we are permuting the last $n-2$ columns of M. On other hand, multiplying M by ${P'}^{-1}$ on the left we are permuting the last $n-2$ rows of M. Hence, we have

$${P'}^{-1}\tau_{e_i}P' = {P'}^{-1}M_{e_i}P'\sigma_{e_iP'} = \tau'_{e_iP'} = \tau'_{e_i\pi}$$

where π is the index permutation induced by P', thus ${P'}^{-1}\mathcal{T}P' = \mathcal{T}'$. This implies that two groups corresponding to vectors with the same weight are conjugated.

Let us now assume that

$$B = (\underbrace{1,\dots,1}_{i},0,\dots,0) \text{ and } B' = (\underbrace{1,\dots,1}_{i+1},0,\dots,0),$$

for some $1 \le i \le n-3$. Let $P \in (\mathbb{F}_2)^{n\times n}$ be the matrix whose j-th row $P_j = e_j$ if $j \ne i+2$ and $P_{i+2} = e_{i+2} + e_{i+3}$, i.e.

$$P \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 & & 0 & \dots & 0 \\ 0 & 1 & & 0 & \dots & 0 \\ \vdots & \vdots & & & & 0 \\ 0 & \dots & 1 & 1 & \dots & 0 \\ 0 & \dots & 0 & 1 & \dots & 0 \\ 0 & 0 & & & \dots & 1 \end{pmatrix}.$$

Note that $P^{-1} = P$. Note also that multiplying a matrix M by P on the right we are updating its $(i+3)$-th column by summing up its $(i+2)$-th and $(i+3)$-th columns. On the other hand, multiplying a matrix M by $P^{-1} = P$ on the left we are updating its $(i+2)$-th row by summing up its $(i+2)$-th and $(i+3)$-th rows. Therefore

$$P\tau_{e_j}P = PM_{e_j}P\sigma_{e_jP} = \tau'_{e_j}$$

for $j \ne i+2$ and

$$P\tau_{(e_{i+2}+e_{i+3})}P = \tau'_{e_{i+2}}.$$

Notice that the group

$$\langle \tau_{e_1}, \dots, \tau_{e_{i+1}}, \tau_{(e_{i+2}+e_{i+3})}, \tau_{e_{i+3}}, \dots, \tau_{e_n} \rangle$$

is exactly $\mathcal{T}$, as $\tau_{(e_{i+2}+e_{i+3})}\tau_{e_{i+3}} = \tau_{e_{i+2}}$. Therefore $P\mathcal{T}P = \mathcal{T}'$. We have also proved that, if B and B' are such that the difference of their Hamming weights is one, by arguments previously used, the associated groups $\mathcal{T}$ and $\mathcal{T}'$ are conjugated in $\mathrm{GL}(V)$.

To conclude, let us address the general case, i.e. the case of two groups obtained by two vectors B and B' having Hamming weight d_1 and d_2. Let us assume, without loss of generality, $d_1 < d_2$. Let us define

$$B_0 \stackrel{\text{def}}{=} (\underbrace{1, \dots, 1}_{d_1}, 0, \dots, 0),\ B_1 \stackrel{\text{def}}{=} (\underbrace{1, \dots, 1}_{d_1+1}, 0, \dots, 0),$$
$$\dots,\ B_{d_2-d_1} \stackrel{\text{def}}{=} (\underbrace{1, \dots, 1}_{d_2}, 0, \dots, 0),$$

and denote by $\mathcal{T}(B_0), \mathcal{T}(B_1), \dots, \mathcal{T}(B_{d_2-d_1})$ the corresponding groups. Reasoning as above, we have that $\mathcal{T}$ and $\mathcal{T}(B_0)$ are conjugated in $\mathrm{GL}(V)$ since B and B_0 have the same Hamming weight, and the same can be proved for $\mathcal{T}'$ and $\mathcal{T}(B_{d_2-d_1})$. Moreover, from a previous argument $\mathcal{T}(B_i)$ is conjugated in $\mathrm{GL}(V)$ to $\mathcal{T}(B_{i+1})$, for each $0 \le i \le d_2 - d_1 - 1$. Therefore, $\mathcal{T}$ and $\mathcal{T}'$ are conjugated in $\mathrm{GL}(V)$, which is our claim. □

4.2. Conjugacy classes in low dimension

In this last section we will focus on spaces with low dimension, i.e. with dimension up to 6. From Proposition 4.2 we obtain the following corollary.

Corollary 4.11. *If* $\dim(V) \le 6$*, then* $T_+ \subseteq \mathrm{AGL}(V, \circ)$ *if and only if* $T_\circ \subseteq \mathrm{AGL}(V, +)$.

The bound of the previous result is tight, as shown below.

Proposition 4.12. *Let* V *be such that* $\dim(V) \ge 7$*. Then there exists an elementary abelian regular subgroup* $T_\circ < \mathrm{AGL}(V, +)$ *such that* $\mathrm{AGL}(V, \circ)$ *does not contain* T_+.

Proof. Let $n \ge 7$ be the dimension of V. If $n > 7$, let us decompose V as $V = V_1 \oplus V_2$, where

$$V_1 \stackrel{\text{def}}{=} \mathrm{Span}\{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$$

and

Table 1
Conjugacy classes.

n	# of classes	classes size	$\dim(W(T_\circ))$
3	2	$\lvert\mathcal{C}_1\rvert = 1$	3
		$\lvert\mathcal{C}_2\rvert = 7$	1
4	2	$\lvert\mathcal{C}_1\rvert = 1$	4
		$\lvert\mathcal{C}_2\rvert = 105$	2
5	4	$\lvert\mathcal{C}_1\rvert = 1$	5
		$\lvert\mathcal{C}_2\rvert = 1085$	3
		$\lvert\mathcal{C}_3\rvert = 6510$	2
		$\lvert\mathcal{C}_4\rvert = 868$	1
6	8	$\lvert\mathcal{C}_1\rvert = 1$	6
		$\lvert\mathcal{C}_2\rvert = 9765$	4
		$\lvert\mathcal{C}_3\rvert = 234360$	3
		$\lvert\mathcal{C}_4\rvert = 410130$	3
		$\lvert\mathcal{C}_5\rvert = 820260$	2
		$\lvert\mathcal{C}_6\rvert = 218736$	2
		$\lvert\mathcal{C}_7\rvert = 54684$	2
		$\lvert\mathcal{C}_8\rvert = 1093680$	2

$$V_2 \stackrel{\text{def}}{=} \mathrm{Span}\{e_8, \dots, e_n\},$$

otherwise we consider only V_1. Let us impose over V_1 the algebra structure induced by the exterior algebra over a vector space of dimension 3, which is the one defined by

$$e_1 \wedge e_2 = e_4, e_1 \wedge e_3 = e_5, e_2 \wedge e_3 = e_6, e_1 \wedge e_2 \wedge e_3 = e_7,$$

and over V_2 the algebra structure given by the trivial product $x * y \stackrel{\text{def}}{=} 0$ for each $x, y \in V_2$. Hence we can define the following product over V:

$$v \cdot w = (v_1 + v_2) \cdot (w_1 + w_2) \stackrel{\text{def}}{=} (v_1 \wedge w_1 + v_2 * w_2) = v_1 \wedge w_1,$$

where $v_1, w_1 \in V_1$ and $v_2, w_2 \in V_2$. It is easy to check that $(V, +, \cdot)$ is a commutative associative $\mathbb{F}_2$-algebra such that the resulting ring is radical. From Theorem 3.1, such an algebra corresponds to an elementary abelian regular subgroup $T_\circ$ of $\mathrm{AGL}(V, +)$. The claim follows from Lemma 3.10 and from its consequences, since $e_1 \cdot e_2 \cdot e_3 \neq 0$. $\square$

Let us now give a classification of all the elementary abelian regular subgroups of $\mathrm{AGL}(V, +)$ up to dimension 6, considering only the relevant cases when $2 < \dim(V) \leq 6$. The results, summarised in Table 1, derive from Corollary 4.8 and Corollary 4.9 and from some computation performed using MAGMA [12]. For each admissible value of n, we collect in Table 1 the number of conjugacy classes of elementary abelian regular subgroups $T_\circ < \mathrm{AGL}(V, +)$, the number of such subgroups in each class and the corresponding dimension of $W(T_\circ)$.

Acknowledgments

Part of the results of this paper are contained in Marco Calderini's Ph.D. thesis [14], supervised by Massimiliano Sala. The authors gratefully thank the referee for comments and recommendations which helped to improve the quality of the paper.

References

[1] F. Abazari, B. Sadeghiyan, Cryptanalysis with ternary difference: applied to block cipher PRESENT, Int. J. Inf. Electron. Eng. 2 (3) (2012) 441.
[2] R. Aragona, M. Calderini, R. Civino, M. Sala, I. Zappatore, Wave-shaped round functions and primitive groups, Adv. Math. Commun. 13 (1) (2019) 67.
[3] R. Aragona, M. Calderini, A. Tortora, M. Tota, Primitivity of PRESENT and other lightweight ciphers, J. Algebra Appl. 17 (06) (2018) 1850115.
[4] R. Aragona, A. Caranti, M. Sala, The group generated by the round functions of a GOST-like cipher, Ann. Mat. Pura Appl. (1923-) 196 (1) (2017) 1–17.
[5] R. Aragona, R. Civino, N. Gavioli, C. Maria Scoppola, Regular subgroups with large intersection, Ann. Mat. Pura Appl. (1923-) 198 (6) (2019) 2043–2057.
[6] R. Aragona, A. Meneghetti, Type-preserving matrices and security of block ciphers, Adv. Math. Commun. 13 (2) (2019) 235.
[7] T.A. Berson, Differential cryptanalysis mod 2^{32} with applications to MD5, in: Workshop on the Theory and Application of Cryptographic Techniques, Springer, 1992, pp. 71–80.
[8] E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, J. Cryptol. 4 (1) (1991) 3–72.
[9] E. Biham, A. Shamir, Differential cryptanalysis of Feal and N-hash, in: Workshop on the Theory and Application of Cryptographic Techniques, Springer, 1991, pp. 1–16.
[10] E. Biham, A. Shamir, Differential cryptanalysis of the full 16-round DES, in: Annual International Cryptology Conference, Springer, 1992, pp. 487–496.
[11] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, C. Vikkelsoe, PRESENT: an ultra-lightweight block cipher, in: International Workshop on Cryptographic Hardware and Embedded Systems, Springer, 2007, pp. 450–466.
[12] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: the user language, J. Symb. Comput. 24 (3–4) (1997) 235–265.
[13] C. Brunetta, M. Calderini, M. Sala, On hidden sums compatible with a given block cipher diffusion layer, Discrete Math. 342 (2) (2019) 373–386.
[14] M. Calderini, On Boolean functions, symmetric cryptography and algebraic coding theory, PhD thesis, University of Trento, 2015.
[15] M. Calderini, M. Sala, On differential uniformity of maps that may hide an algebraic trapdoor, in: International Conference on Algebraic Informatics, Springer, 2015, pp. 70–78.
[16] A. Caranti, F. Dalla Volta, M. Sala, Abelian regular subgroups of the affine group and radical rings, Publ. Math. (Debr.) 69 (3) (2006) 297–308.
[17] A. Caranti, F. Dalla Volta, M. Sala, On some block ciphers and imprimitive groups, Appl. Algebra Eng. Commun. Comput. 20 (5–6) (2009) 339–350.
[18] F. Catino, I. Colazzo, P. Stefanelli, On regular subgroups of the affine group, Bull. Aust. Math. Soc. 91 (1) (2015) 76–85.
[19] F. Catino, R. Rizzo, Regular subgroups of the affine group and radical circle algebras, Bull. Aust. Math. Soc. 79 (1) (2009) 103–107.
[20] R. Civino, C. Blondeau, M. Sala, Differential attacks: using alternative operations, Des. Codes Cryptogr. 87 (2–3) (2019) 225–247.
[21] D. Coppersmith, E. Grossman, Generators for certain alternating groups with applications to cryptography, SIAM J. Appl. Math. 29 (4) (1975) 624–627.
[22] J. Daemen, V. Rijmen, The Design of Rijndael: AES-the Advanced Encryption Standard, Springer Science & Business Media, 2013.
[23] J.D. Dixon, Maximal Abelian subgroups of the symmetric groups, Can. J. Math. 23 (3) (1971) 426–438.
[24] P. Hegedus, Regular subgroups of the affine group, J. Algebra 225 (2) (2000) 740–742.

[25] M. Matsui, Linear cryptanalysis method for DES cipher, in: Workshop on the Theory and Application of Cryptographic Techniques, Springer, 1993, pp. 386–397.
[26] K.G. Paterson, Imprimitive permutation groups and trapdoors in iterated block ciphers, in: Lars Knudsen (Ed.), Fast Software Encryption, Springer Berlin Heidelberg, Berlin, Heidelberg, 1999, pp. 201–214.
[27] M.A. Pellegrini, M.C. Tamburini Bellani, More on regular subgroups of the affine group, Linear Algebra Appl. 505 (2016) 126–151.
[28] M.A. Pellegrini, M.C. Tamburini Bellani, Regular subgroups of the affine group with no translations, J. Algebra 478 (2017) 410–418.
[29] R. Sparr, R. Wernsdorf, Group theoretic properties of Rijndael-like ciphers, Discrete Appl. Math. 156 (16) (2008) 3139–3149.
[30] W.C. Waterhouse, Introduction to Affine Group Schemes, vol. 66, Springer Science & Business Media, 2012.
[31] R. Wernsdorf, The one-round functions of the DES generate the alternating group, in: Workshop on the Theory and Application of Cryptographic Techniques, Springer, 1992, pp. 99–112.
[32] R. Wernsdorf, The round functions of Rijndael generate the alternating group, in: International Workshop on Fast Software Encryption, Springer, 2002, pp. 143–148.